

Universal Sets and Cover-Free Families

Debjyoti Saharoy*

Xerox Research Centre India, Bangalore, Karnataka, India 560103

Shailesh Vaya

Xerox Research Centre India, Bangalore, Karnataka, India 560103

Abstract

We propose a polynomial time construction of an (n, d) -universal set over alphabet $\Sigma = \{0, 1\}$, of size $d \cdot 2^{d+o(d)} \cdot \log n$. This is an improvement over the size, $d^5 2^{2.66d} \log n$, of an (n, d) -universal set constructed by Bshouty, [1], over alphabet $\Sigma = \{0, 1\}$.

Keywords: (n, d) -universal set, cover-free families, t -covering arrays.

1. Introduction

An (n, d) -universal set \mathcal{U} over an alphabet Σ is a family of vectors, $\mathcal{U} \subseteq \Sigma^n$, such that for any index set $S \subset [n]$, with $|S| = d$, the projection of \mathcal{U} on S contains all possible $|\Sigma|^d$ configurations. Universal sets have universal
 5 appeal in almost all scientific disciplines which have concerns regarding testing, where the particular coordinates whose combinatorial possibilities are to be tested are hidden from the tester. They have been intensively studied in the name of t -coverage arrays and are referred to as universal sets in contemporary combinatorics literature. In this short note, we elucidate a construction of
 10 universal sets using cover free families, for $|\Sigma| = 2$, which implies polynomial time construction of almost optimal size universal sets for $|\Sigma| = 2$. However,

*Corresponding author

Email addresses: debjyoti.saharoy@xerox.com (Debjyoti Saharoy),
shailesh.vaya@xerox.com (Shailesh Vaya)

our construction does not depend on the construction of cover-free families. In the remaining part of this section we formally define an (n, d) -universal set and $(n, (r, s))$ -CFF. And also state the related results on the size of their constructions. In section 2 we give the construction of universal sets in Lemma 1 and prove the size bounds in Theorem 2. In section 3 we point some other consequences of this result.

1.1. (n, d) -Universal Set

An (n, d) -universal set over an alphabet Σ is a set $\mathcal{U} \subseteq \Sigma^n$ such that for every $1 \leq i_1 < i_2 < \dots < i_d \leq n$ and every $(\sigma_1, \dots, \sigma_d) \in \Sigma^d$ there is $\mathbf{a} \in \mathcal{U}$ such that $a_{i_j} = \sigma_j$ for all $j = 1, \dots, d$. If $|\Sigma| = q$, then $U(n, d, q)$ is the size of the smallest (n, d) -universal set over the alphabet Σ . The union bound shows that there is an (n, d) -universal set over an alphabet Σ of size

$$U(n, d, q) \leq dq^d \left(\ln \frac{n}{d} + \ln q \right) = O(dq^d \log n).$$

Obviously, finding a small (n, d) -universal set is a *d-restriction problem* [2]. For $q = 2$, a lower bound of $\Omega(2^d \log n)$ was proved in [3]. The polynomial time (i.e $\text{poly}(q^d, n)$) construction for this problem of size $d^{O(\log d / \log q)} q^d \log n$ for $q < d$, [2], [4], was improved by Bshouty [1]. Specifically, for $q = 2$, [1] gave a polynomial time construction of (n, d) -universal set of size not exceeding $d^5 2^{2.66d} \log n$.

1.2. Cover-Free Family

Let us fix positive integers r, s, n with $r, s < n$ and let $d := r + s$. Let X be a set with N elements and let \mathcal{B} be a set of subsets (blocks) of X , $|\mathcal{B}| = n$. Then (X, \mathcal{B}) is a $(n, (r, s))$ -cover-free family $((n, (r, s))$ -CFF), [5], if for any r blocks $B_1, \dots, B_w \in \mathcal{B}$ and any other s blocks $A_1, \dots, A_r \in \mathcal{B}$, we have

$$\bigcap_{i=1}^r B_i \not\subseteq \bigcup_{j=1}^s A_j.$$

Equivalently, given an $(n, (r, s))$ -CFF \mathcal{F} , denote $N = |\mathcal{F}|$ and construct the $N * n$ boolean matrix A whose rows are the elements of \mathcal{F} and the columns

can be thought of as the characteristic vectors of subsets. If $\mathcal{B} = B_1, \dots, B_n$ denotes the set of blocks corresponding to the columns, then A is the incidence
 30 matrix of \mathcal{B} , i.e. the i^{th} element of X is in B_j iff $A_{i,j} = 1$.

The CFF property of \mathcal{F} implies that for any r blocks $B_1, \dots, B_r \in \mathcal{B}$ and any other s blocks $A_1, \dots, A_s \in \mathcal{B}$ (distinct from the B 's), there is an element of X contained in all the B 's but not in any of the A 's. Let $N(n, (r, s))$ denote the minimum size of any $(n, (r, s))$ -CFF.

D'yachkov et. al.'s breakthrough result, [6], implies that for $s, n \rightarrow \infty$

$$N(n, (r, s)) = \Theta(N(r, s) \cdot \log n). \quad (1)$$

where

$$N(r, s) := \frac{d \binom{d}{r}}{\log \binom{d}{r}}.$$

This bound is non-constructive. Bshouty et. al., [7] calls an $(n, (r, s))$ -CFF \mathcal{F} *almost optimal*, if it's size $N = |\mathcal{F}|$ satisfies

$$N = N(r, s)^{1+o(1)} \cdot \log n$$

and for $r = O(d)$

$$N = N(r, s)^{1+o(1)} \cdot \log n = 2^{H_2(r/d)d+o(d)} \cdot \log n \quad (2)$$

35 where $H_2(x)$ is the binary entropy function. The term $o(1)$ is independent of n and tends to 0 as $d \rightarrow \infty$. A CFF family \mathcal{F} is said to be constructed in linear time if it can be constructed in time $O(N(r, s)^{1+o(1)} \cdot \log n \cdot n)$.

Bshouty [1, 8] and Bshouty et. al. [7] constructed almost optimal $(n, (r, s))$ -CFF \mathcal{F} for $r < d^{o(1)}$ and $d^{o(1)} < r < \omega(d/(\log \log d \log \log \log d))$ respectively,
 40 in linear time. Fomin et. al. [9] constructed almost optimal $(n, (r, s))$ -CFF \mathcal{F} for $r > \omega(d/(\log \log d \log \log \log d))$ in linear time.

2. Construction of Universal Sets

We give the explicit (i.e polynomial time) construction of (n, d, q) -universal set \mathcal{U} , for $q = 2$, using $(n, (r, s))$ -CFF \mathcal{F} . We use the explicit linear time
 45 construction of almost optimal size $(n, (r, s))$ -CFF \mathcal{F} given in [1, 7, 8, 9].

Notation: Let us denote an (n, d, q) -universal set \mathcal{U} by $\mathcal{U}_{(n,d,q)}$. We suppress q , if $q = 2$. We denote an $(n, (r, s))$ -CFF \mathcal{F} by $\mathcal{F}_{(n,(r,s))}$. Our construction is based on the following lemma.

Lemma 1.

$$\mathcal{U}_{(n,d)} = \bigcup_{i=0}^{d-1} \mathcal{F}_{(n,(i,d-i))} \quad (3)$$

$\mathcal{U}_{(n,d)}$ is an (n, d) -universal set over alphabet $\Sigma = \{0, 1\}$. If $N(n, (d/2, d/2))$ denotes the size of an optimal $(n, (d/2, d/2))$ -CFF, then $|\mathcal{U}_{(n,d)}| \leq d \cdot N(n, (d/2, d/2))$.
 Moreover, $|\mathcal{U}_{n,d}|$ is in asymptotic equivalence with $N(n, (r, s))$ for $r = O(d)$.

Proof. First we prove that $\mathcal{U}_{(n,d)}$ is indeed an (n, d) -universal set. The proof is by contradiction. Let us assume that exists some $1 \leq i_1 < i_2 < \dots < i_k \leq n$ and $(\sigma_1, \dots, \sigma_d) \in \Sigma^d$ such that for no $a \in \mathcal{U}_{(n,d)}$, $a_{i_j} = \sigma_j$ for all $j = 1 \dots, d$.
 Without loss of generality, let us assume that the chosen $(\sigma_1, \dots, \sigma_d)$ has r 1's and s 0's where $r + s = d$. In other words, the $(\sigma_1, \dots, \sigma_d) \notin \mathcal{F}_{(n,(r,s))}$. This is not possible by the definition of $(n, (r, s))$ -CFF \mathcal{F} . Hence the contradiction.

We now calculate the size of the $\mathcal{U}_{(n,d)}$.

$$\begin{aligned} |\mathcal{U}_{(n,d)}| &= \left| \bigcup_{i=0}^{d-1} \mathcal{F}_{(n,(i,d-i))} \right| \\ &= 2 \cdot \left| \bigcup_{i=0}^{\frac{d}{2}-1} \mathcal{F}_{(n,(i,d-i))} \right| \\ &\leq d \cdot N(n, (d/2, d/2)) \end{aligned} \quad (4)$$

The second equality follows from the fact that we can consider $r \leq d/2$, because if not, one can construct an $\mathcal{F}_{(n,(s,r))}$ and take the set of complement vectors. The first inequality follows from the fact that the size of $\mathcal{F}_{(n,(r,s))}$ for $r = O(d)$ dominates $r = O(1)$, $r = \omega(1)$ and $r = o(d)$. It must be noted that the bound on the size of $\mathcal{U}_{(n,d)}$ is in asymptotic equivalence with bound on the size of an $(n, (r, s))$ -CFF \mathcal{F} for $r = O(d)$. We can claim so because any *optimal* or *almost optimal* construction of an $(n, (r, s))$ -CFF \mathcal{F} must obey the tight bound given by D'yachkov et. al, [6], in eq. (1), and the bound (i.e the quantity

$N(n, (r, s))$ in eq. (1) is monotonically increasing in d .

□

Bshouty, [1], constructed an (n, d) -universal set of size $d^5 2^{2.66d} \log n$ over an alphabet $\Sigma = \{0, 1\}$. To the best of our knowledge this is the best polynomial
70 time construction for this problem over an alphabet of size 2. We give the following theorem which improves this size.

Theorem 2. $\mathcal{U}_{n,d}$ is an explicitly (i.e in polynomial time) constructed (n, d) -universal set over alphabet $\Sigma = \{0, 1\}$, of size $d \cdot 2^{d+o(d)} \cdot \log n$.

Proof. Using inequality (4) and almost optimal construction of an $(n, (r, s))$ -CFF by [1, 7, 8, 9] for $r = O(d)$,

$$\begin{aligned} |\mathcal{U}_{(n,d)}| &\leq d \cdot N(n, (d/2, d/2)) \\ &= d \cdot N(d/2, d/2)^{1+o(1)} \cdot \log n \\ &= d \cdot 2^{H_2(1/2)d+o(d)} \cdot \log n \\ &= d \cdot 2^{d+o(d)} \cdot \log n \end{aligned}$$

The first equality follows from eq. (2). The polynomial time taken in the
75 construction follows from the fact that we take the union of d , $(n, (d/2, d/2))$ -CFF each of which is constructed in linear time.

□

Remark 1. We also make the observation that the construction of $(n, d, 2)$ -universal set in Lemma 1 can also be extended for small q 's greater than 2 (like
80 $q = 3, 4$) by adapting Colbourn et. al.'s, [10], construction of product of covering arrays.

3. Some Consequences of (n, d) -Universal Set

The improved construction of the (n, d) -universal set have direct consequences in the problem of fault-tolerance of an hypercube, [11]. It also im-
85 proves the running time of Blum and Rudich's, [12], learning algorithm for k -term DNFs as well as Bshouty's, [13], learning algorithm for k -CNF. As pointed

out by Naor in [2], improved construction of universal sets also improves the non-approximability results of the *set cover* problem. It also finds application in distributed colouring: provides a constructive argument of the existence of
90 recoloring protocols of Szegedy and Vishwanathan [14].

References

- [1] N. Bshouty, Testers and their applications, in: Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, ITCS '14, ACM, New York, NY, USA, 2014, pp. 327–352.
- 95 [2] M. Naor, L. J. Schulman, A. Srinivasan, Splitters and near-optimal derandomization, in: Foundations of Computer Science, 1995. Proceedings., 36th Annual Symposium on, IEEE, 1995, pp. 182–191.
- [3] D. J. Kleitman, J. Spencer, Families of k -independent sets, Discrete Mathematics 6 (3) (1973) 255 – 262.
- 100 [4] N. Alon, J. Bruck, J. Naor, M. Naor, R. M. Roth, Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs, Information Theory, IEEE Transactions on 38 (2) (1992) 509–516.
- [5] W. H. Kautz, R. C. Singleton, Nonrandom binary superimposed codes, Information Theory, IEEE Transactions on 10 (4) (1964) 363–377.
- 105 [6] A. G. D'yachkov, I. V. Vorob'ev, N. A. Polyansky, V. Y. Shchukin, Bounds on the rate of disjunctive codes, Problems of Information Transmission 50 (1) (2014) 27–56.
- [7] N. H. Bshouty, A. Gabizon, Almost optimal cover-free families, CoRR abs/1507.07368.
- 110 [8] N. H. Bshouty, Linear time constructions of some $\$d\$$ -restriction problems, CoRR abs/1406.2108.

- [9] F. V. Fomin, D. Lokshantov, S. Saurabh, Efficient computation of representative sets with applications in parameterized and exact algorithms, in: Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '14, SIAM, 2014, pp. 142–151.
- [10] C. J. Colbourn, S. S. Martirosyan, G. L. Mullen, D. Shasha, G. B. Sherwood, J. L. Yucas, Products of mixed covering arrays of strength two, Journal of Combinatorial Designs 14 (2) (2006) 124–138.
- [11] G. Seroussi, N. H. Bshouty, Vector sets for exhaustive testing of logic circuits, Information Theory, IEEE Transactions on 34 (3) (1988) 513–522.
- [12] B. Berger, J. Rompel, Simulating $(\log n)$ -wise independence in nc , in: Foundations of Computer Science, 1989., 30th Annual Symposium on, 1989, pp. 2–7.
- [13] N. H. Bshouty, Exact learning via the monotone theory, in: Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on, IEEE, 1993, pp. 302–311.
- [14] M. Szegedy, S. Vishwanathan, Locality based graph coloring, in: Proceedings of the twenty-fifth annual ACM symposium on Theory of computing, ACM, 1993, pp. 201–207.